



Routing Without Rumor: Securing the Internet's Routing System

Dr. Burt Kaliski, Sr. Vice President and CTO

March 22, 2022

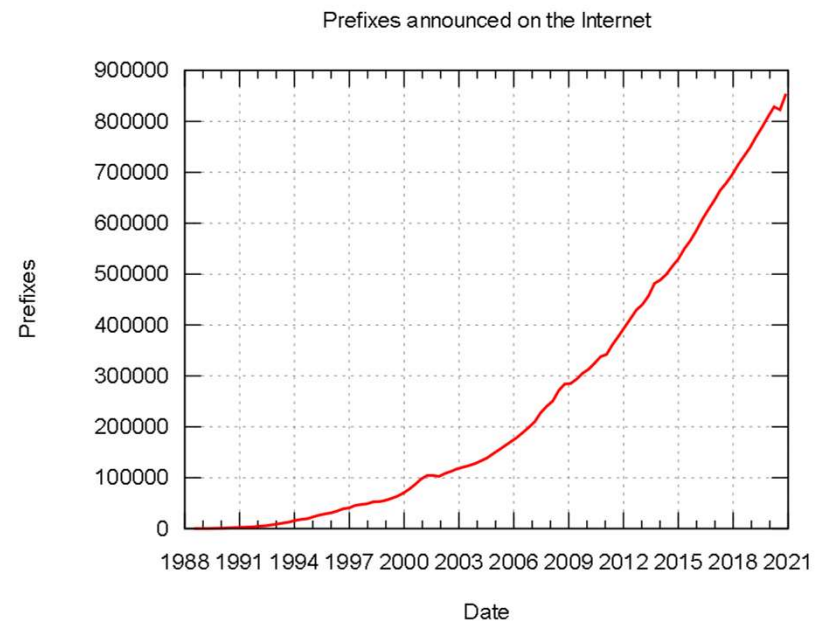
Verisign Public

Routing by Rumor

- **Internet routing system** is fundamental to internet security, stability and resiliency
 - What are the available routes to internet destinations?
- Effective, robust, immense scale
- Decentralized, implicit trust model
- Networks share knowledge of routes with one another ...
they **route by rumor**

Border Gateway Protocol (BGP)

- **BGP** is the internet's routing protocol
 - RFC 1105 in 1989; RFC 4271 for v4 in 2006
- Networks route traffic based on local policy using shared knowledge of routing paths
- No central point of control — or failure



< 100,000 global routes in 2000



> 850,000 global routes in 2021

Source: Mro / Bombenleger, CC BY-SA 3.0

Route Hijacks and Leaks

- **Route hijacks** divert traffic to an *unintended destination*
- **Route leaks** draw traffic through an *unintended path*
- *Millions* of events reported;
15 major events since 2017
 - Average duration: 1h 57m

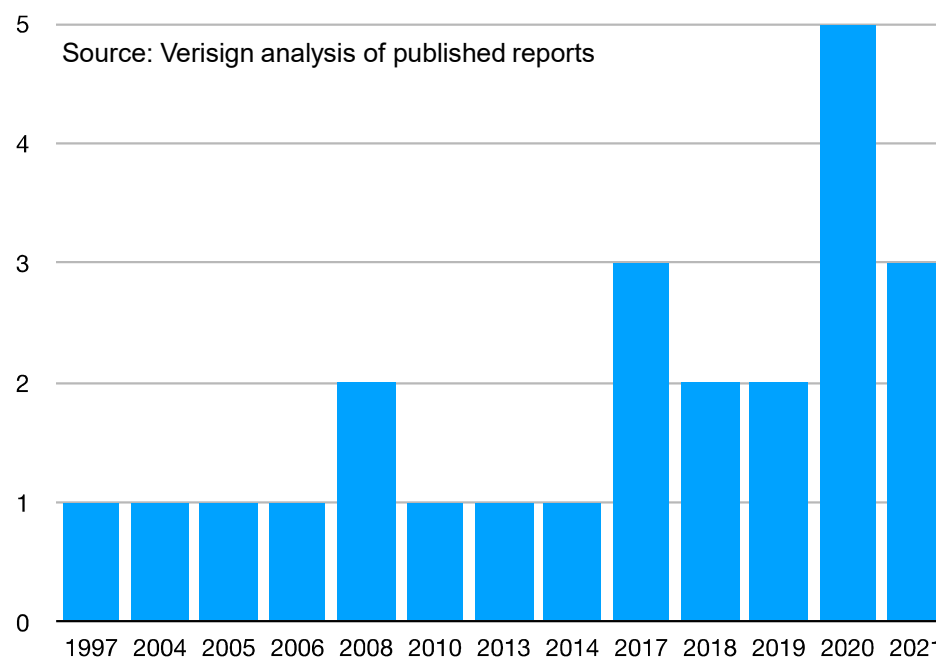


Couple of DNS servers were hijacked to resolve myetherwallet.com users to be redirected to a phishing site. This is not on [@myetherwallet](https://twitter.com/myetherwallet) side, we are in the process of verifying which servers to get it resolved asap.

8:29 AM · Apr 24, 2018



Public BGP Hijacks



Resource Public Key Infrastructure (RPKI)

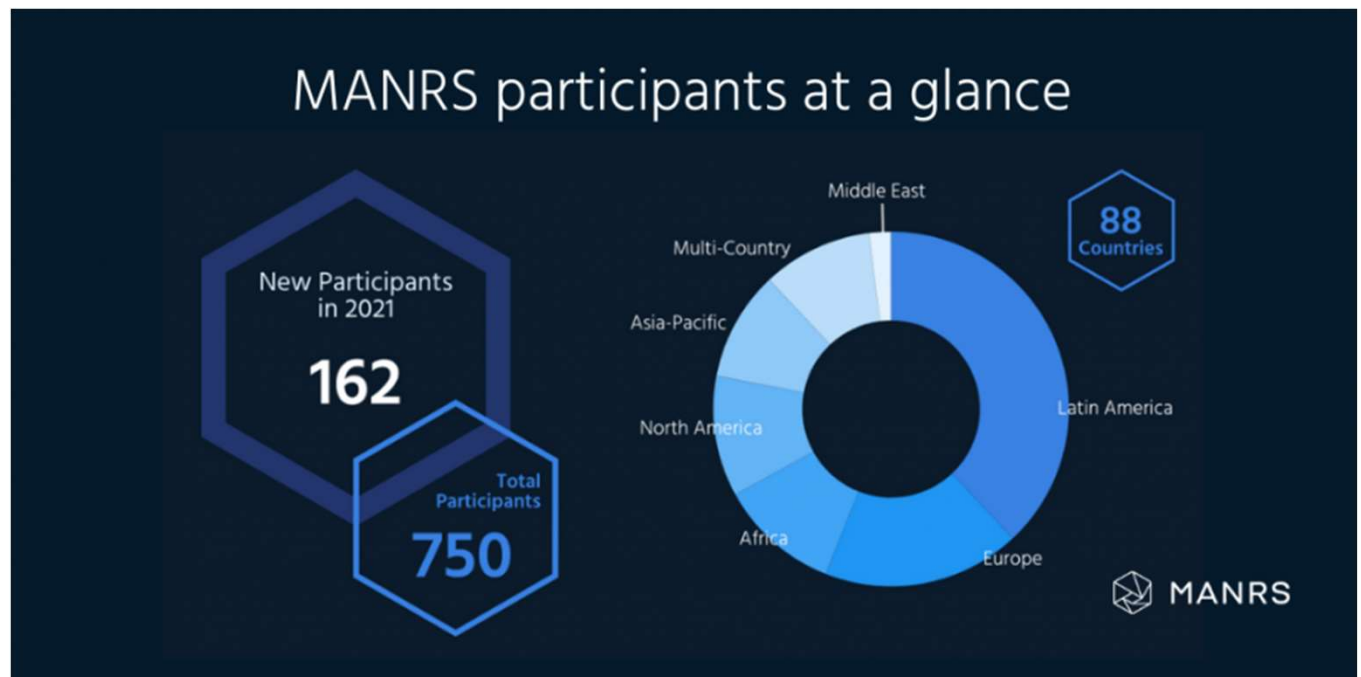
- **RPKI** enables networks to **validate route origins**
 - RPKI: RFCs 6480-6495 in 2012
- Centralized, explicit trust model for authorization information
- ... but new critical dependencies
- Technical details ...
 - Regional Internet Registries provide trust anchors, issue Route Origin Authorizations (ROA)
 - ROAs cryptographically associate IP address prefixes with network ASNs
 - Route Origin Validation occurs out-of-band
 - Next: Path validation (draft-ietf-sidrops-aspa-verification)

Mutually Agreed Norms for Routing Security (MANRS)

MANRS is a community-led initiative to improve routing security

Key techniques:

- Coordination
- Global Validation
- Anti-Spoofing
- Filtering



Source: <https://www.manrs.org/isps/guide/>

Source: MANRS.org

Routing without Rumor

- Routing by rumor has served the internet well while avoiding systemic dependencies
- Critical role of internet, evolving cyberthreat landscape require a better approach ... including better “MANRS”
- RPKI offers a first step toward a new approach where networks *verify* routing information ... and **route without rumor**

For more information, please see Danny McPherson’s article, “Routing Without Rumor: Securing the Internet’s Routing System” on Verisign’s blog

powered by



VERISIGN[®]

© 2022 VeriSign, Inc. All rights reserved. VERISIGN and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.